

Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2012 covering the prior calendar year 2011

1. Date filed: January 30, 2012
2. Name of company(s) covered by this certification: W.A.T.C.H. TV Company
3. Form 499 Filer ID: 827573
4. Name of signatory: Thomas N. Knippen
5. Title of signatory: Vice President
6. Certification:

I, Thomas N. Knippen certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

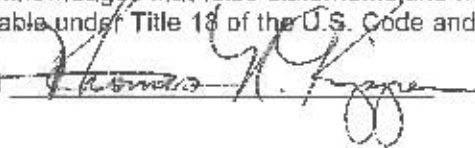
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed



Attachments: Accompanying Statement explaining CPNI procedures
Explanation of actions taken against data brokers (if applicable)
Summary of customer complaints (if applicable)

W.A.T.C.H. TV COMPANY

STATEMENT OF CPNI PROCEDURES

W.A.T.C.H. TV Company has created a CPNI Policy Handbook containing the following procedures that it has adopted to ensure the protection of CPNI. The handbook describes our procedures in greater detail and provides practical guidance on how to protect against unauthorized disclosure or use of CPNI. The handbook is distributed to our employees during training and serves as an important reference tool for our employees.

Duty to Protect CPNI

We as a communications companies recognize our duty to protect customer CPNI. We may not disclose CPNI to unauthorized persons, nor may we use CPNI in certain ways without consent from our customers. Before we can provide customers with their own CPNI, we must authenticate the customer.

We recognize that there are a few cases in which we can disclose CPNI without first obtaining customer approval:

1. Administrative use: We may use CPNI to *initiate, render, bill and collect for* communications services.
2. Protection of carrier and third parties: We may use CPNI to protect the interests of our companies, such as to prevent fraud or illegal use of our systems and network. Employees are notified of the steps to take, if any, in these sorts of situations.
3. As required by law: We may disclose CPNI if we are required to by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Employees are notified of any steps they must take in these situations.

Our Own Use Of CPNI

We may use CPNI to provide or market services to our existing customers. We understand that we are required to obtain customer approval prior to using CPNI in certain ways.

Marketing

We understand that we do not need to obtain customer approval before using CPNI to market services to our existing customers within the categories of service to which the customer already subscribes.

We understand that we may not use CPNI to market services that are in a service category to which the customer does not already subscribe without customer approval.

We understand that we cannot use CPNI to solicit a customer to add a new category of service without first obtaining the customer's approval.

We also understand that we do not need customer consent before using CPNI to market "adjunct-to-basic" services such as speed dialing, computer-provided directory assistance, call monitoring, call

Mail

If the customer requests CPNI through regular mail, or if the customer cannot comply with one of the authentication methods above, we send the requested information to the customer's address of record only.

Online Access

At this time, we offer online account access to our VoIP customers only. We password protect online access to CPNI. All existing customers have established passwords, and new customers establish passwords at service initiation. We do not allow customers to choose passwords based on their readily available biographical information or account data.

After a customer has made 3 failed attempts to log into his/her online account, we block online access to the account for security purposes. Customers locked out of their online accounts must present photo identification at our office to regain online account access. Furthermore, if a customer loses or forgets his/her online account password, the customer must present photo identification at our office to obtain password information for the account.

Customer Notification of CPNI Rights

We provide a CPNI privacy policy to all customers annually, as a bill insert in the December bill. This policy provides notification to each customer of his/her right to restrict use of, disclosure of, and access to that customer's CPNI. We maintain a list of all customers who receive the privacy policy, the date on which the policy is sent, and a copy of the policy in our records for one (1) year following the mailing of the policy. We provide additional copies of the CPNI privacy policy to all customers who request it and to all new customers upon activation of service.

The policy contains an opt-out customer approval notice. Customers who do not wish to allow us to use their CPNI to market services outside their existing service categories, or who do not wish to allow us to share their CPNI with affiliates, have 30 days to contact us to tell us that they do not approve of this use. If we do not hear back from the customer within 30 days, we understand that we are free to use their CPNI for these purposes. We understand that customers can change their option at any time by contacting us, and we notify our customers of this right.

We maintain records of the customers who received the opt-out approval notice and records of the customers who contacted us to opt out in accordance with our record-keeping policies.

We understand that we must provide written notice to the FCC within five (5) business days if our opt-out mechanisms do not work properly to the degree that our customers' inability to opt out is more than an anomaly.

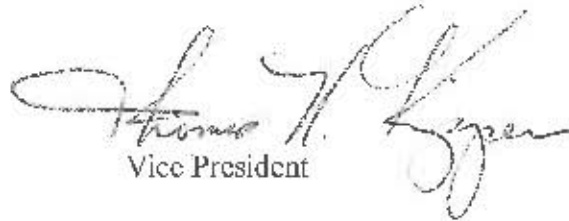
Training And Discipline

We trained all of our employees regarding the company's CPNI policies prior to the effective date of the most recent CPNI regulations, December 8, 2007. Employees are required to attend an annual retraining to ensure that they understand the companies' CPNI policies and any updates to those policies. New employees who will have access to CPNI are trained when they join the companies, and then attend the regularly-scheduled retraining sessions. At the conclusion of each training session, employees are

(iii) a detailed description of the CPNI breached, and (iv) the circumstances of the breach.

During the course of the year, we compile information regarding pretexter attempts to gain improper access to CPNI, including any breaches or attempted breaches. We include this information in our annual CPNI compliance certification filed with the FCC.

Signed


Vice President